5. **SECURITY RISK ASSESSMENTS AND DESIGN REVIEWS** - The Contractor shall complete a security risk assessment on a design prior to the design being provided to NASA. Before or during official design review, the Contractor shall provide design security risks, including possible mitigations, to the system owner or data owner. If the risks are accepted the life cycle may continue, otherwise the life cycle shall halt or the design and/or mitigations shall be modified until the risks and possible mitigations are acceptable.

6. **SECURITY REVIEWS FOR NEW OR MODIFIED HARDWARE AND SOFTWARE** - The Contractor shall provide a written risk assessment and security review for new or significantly modified hardware or software, prior to deployment (page 21 last paragraph of NIST 800-37). The products reviewed shall be used as a basis to update IT Security Plans, as applicable. Prior to deployment, all risks shall be presented to the system owner or equivalent, separate from the security plan. If the hardware or software connects to other systems the risks shall be presented to the system owner or equivalents of the interconnected systems for their information.

7. **STORAGE OF SYSTEM DOCUMENTATION** - The Contractor shall store duplicate copies of system documentation, including updates, in accordance with section 11.

8. **PROHIBITION OF PRODUCTION DATA ON NON-PRODUCTION NETWORKS** - The Contractor shall not store, copy, or transfer NASA sensitive but unclassified (SBU) data to any non certified and accredited (C&A) system, IAW NPR 2810.1*x* or for non NASA system IAW NIST 800-37.

9. **DISTRIBUTION OF RISKS, THREATS AND VULNERABILITIES** - The Contractor shall encrypt all electronic transmissions of SBU information.

10. **OPERATIONAL CONTROLS**

    a. System Contingency Planning

       i. CONTINGENCY PLANNING AND EMERGENCY PREPAREDNESS - The Contractor shall participate in contingency and Disaster Recovery (DR) planning, training, and testing in accordance with the current Center Contingency Plan.

       ii. The Contractor shall at least annually train contingency teams in plan procedures and operations. The Contractor shall at least annually develop, plan, and implement a contingency scenario test designed to validate the effectiveness of the plan to quickly restore IT operations in the event of a disaster. The Contractor shall deliver a lessons learned report from each test and use the results to update the IT Contingency Plan.

       iii. In the event the Center's plan is invoked, the Contractor shall participate in Center DR operations in accordance with the Center Contingency and DR Plan.

    b. System Monitoring

       i. IT Security Audits, Assessments, Certifications, Bulletins and Alerts. The Contractor shall provide all necessary support in the event of a Government-initiated investigation, Assessment or Certification involving the Contractor's team or the Contractor's customers. Also, the Contractor shall provide all services necessary to properly respond to NASA IT security bulletins or notices from the NASA Incident Response Center (NASIRC), or the NASA Chief Information Officer that apply to any Contractor-supported system or environment. The Contractor shall take necessary and/or immediate corrective actions on ODIN seats in response to these bulletins and notices, and shall notify the system owner or DOCOTR or designee of any suspicious activities per Center security procedures. Audits, investigations, and emergency corrective actions may be initiated by the Office of Inspector General (OIG); Office of Management and Budget (OMB); Government Accounting Office (GAO); Federal Bureau of Investigation (FBI); or the Center's IT Security Manager, Chief Information

Officer; Chief Counsel; Head of Human Capital, or others as directed by the system owner or DOCOTR.

11. **BACKUP MEDIA** - The Contractor shall log removals of all backup media for multi-user systems. The Contractor shall maintain separation of duties while accessing and transporting backup media outside the NASA Center. The Contractor shall store backup media at an off-site location secure from threats.

12. TECHNICAL CONTROLS

Authorization Process for Network Access: In accordance with NPR 2810.1*x* and NPR 1600.1, the Contractor shall grant no network access, beyond the OSI Data Link Layer, without the user following the Center process for requesting and gaining approval for such network access. This requirement applies to any ODIN service that involves granting/changing network access, including adding new customers and moves/adds/changes involving existing customers.

a. Vulnerability Monitoring and Reporting

i. The Contractor shall provide IT security vulnerability services that affect all ODIN systems by monitoring/reviewing the following:

- NASIRC distributed bulletins and alerts
- The standard web browser contractor web sites
- The standard E-mail client web site
- The operating system web sites for MACs, Windows PCs, and other desktops
- Vulnerability scans
- Relevant E-mails from the system owner, DOCOTR and ITSM

ii. When the Contractor finds, or is notified of an ODIN vulnerability, the Contractor shall report an "initial" recommended severity within four business hours via encrypted E-mail or hand delivery (not unencrypted voice).

iii. If initial severity is Critical or High, the Contractor shall immediately contact one of the following in this order for concurrence on severity:

- The system owner
- DOCOTR
- Center IT Security Manager
- Center CIO

iv. The following conditions shall be used to determine initial severity:

- CRITICAL (A1 plus one of B plus one of C)
- HIGH (A1 plus one of B OR A1 plus both of C)
- MEDIUM (A2 plus one of B OR A2 plus both of C)
- LOW any other vulnerability, i.e., one that provides information that could affect availability, confidentiality, or integrity.

A	B	C
1. Affects availability, confidentiality or integrity of center border systems or internal systems from external network sources 2. All other vulnerabilities on HQ border systems or internal systems	1. A known scripting exploit exists 2. The vulnerability can be easily exploited by non-scripting or manual means (easy to exploit) 3. Probes for this vulnerability have been detected at the border	1. If reported on www.cnn.com, or www.msnbc.com, or if notified that it exists on another widely read normal media site (These sites do not need to be monitored on a normal basis only when vulnerability evaluation occurs and A and B are met) 2. Has been flagged for special attention by senior NASA officials.

b. ODIN System Vulnerability Scanning: In addition to complying with ITS-SOP-0021 requirements, The Contractor shall ensure vulnerability scanning is conducted for each ODIN system according to Center procedures, including, but not limited to:

i. All ODIN servers shall be scanned prior to operational readiness review or full production.

ii. All new ODIN desktop software loads and configurations shall be scanned prior to deployment.

iii. All ODIN systems infected with viruses or malware shall be rescanned after mitigation and prior to redeployment.

iv. Any ODIN system that is compromised via unknown means must be rebuilt from a core load.

c. System Incident Handling and Reporting

i. IT Security Incident Response

For an IT security incident, the Contractor shall report the incident to the ITSM or designee(s) within one (1) hour and shall follow the Center's documented IT security incident response procedures. The Contractor shall use the format and content set forth in each Center's incident response report, DRD Core-8, Standard Reporting for Security Incidents Reports.

Unexplained system anomalies that, in the judgment of the system administrator, may affect confidentiality of data or integrity of a system/data shall be reported to the CITSM or designee within one (1)hour. Such anomalies include, but are not limited to, unexplained change of directory or file permissions, unexplained installation, removal or starting/stopping of software, unexplained network traffic, unexplained unavailability of a production service, or any malicious activity. The Contractor shall provide all necessary assistance to the investigating team.

ii. Security Awareness Training

System Administrator Certification: All ODIN Contractor individuals who perform tasks as a system administrator or have authority to perform tasks normally performed by system administrator shall be required to demonstrate knowledge appropriate to those tasks. This demonstration, referred to as the NASA System Administrator Security Certification (currently a Brainbench certification), is a NASA funded two-tier assessment to verify that system administrators are able to:

1. Demonstrate knowledge in system administration for the operating systems for which they have responsibility.

2. Demonstrate knowledge in the understanding and application of Network and Internet Security.

Certification is granted upon achieving a score above the certification level on both an Operating System test and the Network and Internet Security Test. The Certification earned under this process will be valid for 3 years. The criteria for this skills assessment have been established by the NASA Chief Information Officer. The objectives and procedures for this certification can be obtained by contacting the IT Security Awareness and Training Center at (216) 433-2063.

A system administrator is one who provides IT services, network services, files storage, web services, etc. and takes or assumes the responsibility for the security and administrative controls of that service or machine. A lead system administrator has responsibility for information technology security (ITS) for multiple computers or network devices represented within a system; ensuring all devices assigned to them are kept in a secure configuration (patched/mitigated); and ensuring that all other system administrators under their lead understand and perform ITS duties.

iii. Security Training

As defined in NPR 2810.1*x*, all Contractor personnel with access to government data, including off-site personnel supporting the contract shall complete security training annually as required to meet Agency IT security training and awareness requirements. The Contractor shall report quarterly on status of the required training of their employees. Reports shall be submitted to the DOCOTR or designee.

13. **BACKGROUND INVESTIGATIONS:** Background investigations shall be conducted in accordance with the requirement of NPR 1600.1, to include subcontractors and other personnel supporting the ODIN contract. The background investigations will be conducted by NASA upon submission of the required forms by the Contractor.

14. **NATIONAL SECURITY INFORMATION REQUIREMENTS**: Form DD-254 is hereby incorporated into the Delivery Order as Attachment H.

15. **IT SECURITY REPORTING REQUIREMENTS:** The Contractor shall comply with reporting requirements set by the Federal Information Security Management Act (FISMA), the Office of Management and Budget (OMB), the Office of the Inspector General (OIG), and the Center and Agency CIO as baselined and agreed to at the start of the Delivery Order period of performance. The baseline will be reviewed on an annual basis and as necessary to comply with new policies, requirements, or laws and be re-negotiated only when the reporting requirements exceed the baselined resources.

16. **RESERVED**

17. **RESERVED**

18. **RESERVED**

19. **RESERVED**

20. **RESERVED**

PART IV RESERVED

PART V CORE CLAUSES

The following ADDENDA to FAR 52.212-4 are incorporated:

1. FAR 52.252-2 Clauses Incorporated by Reference (Feb 1998)

The Contractor agrees to comply with the following FAR and NFS clauses, which are incorporated by reference to implement provisions of law or executive orders. FAR clauses are available in full text at: http://acquisition.gov/far. NFS clauses are available in full text at: http://www.hq.nasa.gov/office/procurement/regs/nfstocA.htm.

A. FEDERAL ACQUISITION REGULATION (48 CFR CHAPTER 1)

CLAUSE NO.	DATE	TITLE
52.204-4	AUG 2000	Printed or Copied Double-Sided on Recycled
52.204-7	JUL 2006	Central Contractor Registration
52.204-9	JAN 2006	Personal Identity Verification of Contractor Personnel
52.225-13	FEB 2006	Restrictions on Certain Foreign Purchases
52.232-18	APR 1984	Availability of Funds
52.232-33	OCT 2003	Payment by Electronic Funds Transfer—Central Contractor Registration
52.233-4	OCT 2004	Applicable Law for Breach of Contract Claim

B. NASA/FAR SUPPLEMENT (48 CFR CHAPTER 18)

CLAUSE NO.	DATE	TITLE
1852.219-75	MAY 1999	Small Business Subcontracting Reporting
1852.219-76	JUL 1997	NASA 8 Percent Goal
1852.223-71	DEC 1988	Frequency Authorization
1852.223-73	NOV 2004	Safety and Health Plan
1852.225-70	FEB 2004	Export Licenses (FEB 2000)
1852.237-72	MAY 2005	Access to Sensitive Information
1852.237-73	MAY 2005	Release of Sensitive Information

(End of Clause)

2. 1852.204-76 SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES (NOVEMBER 2004 [(DEVIATION])

(a) The Contractor shall be responsible for information and information technology (IT) security when the Contractor or its subcontractors must obtain physical or electronic (i.e., authentication level 2 and above as defined in NIST Special Publication (SP) 800-63, Electronic Authentication Guideline) access to NASA's computer systems, networks, or IT infrastructure, or where information categorized as low, moderate, or high by the Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, is stored, generated, or exchanged by NASA or on behalf of NASA by a contractor or subcontractor, regardless of whether the information resides on a NASA or a contractor/subcontractor's information system.

(b) IT Security Requirements.

(1) Within 30 days after contract award, a Contractor shall submit to the Contracting Officer for NASA approval an IT Security Plan, Risk Assessment, and FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, Assessment. These plans and assessments, including annual updates shall be incorporated into the contract as compliance documents.

(i) The IT system security plan shall be prepared consistent, in form and content, with NIST SP 800-18, Guide for Developing Security Plans for Federal Information Systems, and any additions/augmentations described in NASA Procedural Requirements (NPR) 2810, Security of Information Technology. The security plan shall identify and document appropriate IT security controls consistent with the sensitivity of the information and the requirements of Federal Information Processing Standards (FIPS) 200, Recommended Security Controls for Federal Information Systems. The plan shall be reviewed and updated in accordance with NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems, and FIPS 200, on a yearly basis.

(ii) The risk assessment shall be prepared consistent, in form and content, with NIST SP 800-30, Risk Management Guide for Information Technology Systems, and any additions/augmentations described in NPR 2810. The risk assessment shall be updated on a yearly basis.

(iii) The FIPS 199 assessment shall identify all information types as well as the "high water mark," as defined in FIPS 199, of the processed, stored, or transmitted information necessary to fulfill the contractual requirements.

(2) The Contractor shall produce contingency plans consistent, in form and content, with NIST SP 800-34, Contingency Planning Guide for Information Technology Systems, and any additions/augmentations described in NPR 2810. The Contractor shall perform yearly "Classroom Exercises." "Functional Exercises," shall be coordinated with the Center CIOs and be conducted once every three years, with the first conducted within the first two years of contract award. These exercises are defined and described in NIST SP 800-34.

(3) The Contractor shall ensure coordination of its incident response team with the NASA Incident Response Center and the NASA Security Operations Center.

(4) The Contractor shall ensure that its employees, in performance of the contract, receive annual IT security training in NASA IT Security policies, procedures, computer ethics, and best practices in accordance with NPR 2810 requirements. The Contractor may use web-based training available from NASA to meet this requirement.

(5) The Contractor shall provide NASA, including the NASA Office of Inspector General, access to the Contractor's and subcontractors' facilities, installations, operations, documentation, databases, and personnel used in performance of the contract. Access shall be provided to the extent required to carry out IT security inspection, investigation, and/or audits to safeguard against threats and hazards to the integrity, availability, and confidentiality of NASA information or to the function of computer systems operated on behalf of NASA, and to preserve evidence of computer crime. To facilitate mandatory reviews, the Contractor shall ensure appropriate compartmentalization of NASA information, stored and/or processed, either by information systems in direct support of the contract or that are incidental to the contract.

(6) The Contractor shall ensure that all individuals who perform tasks as a system administrator, or have authority to perform tasks normally performed by a system administrator, demonstrate knowledge appropriate to those tasks. Knowledge is demonstrated through the NASA System Administrator Security Certification Program. A system administrator is one who provides IT services, network services, files storage, and/or web services, to someone else other than themselves and takes or assumes the responsibility for the security and administrative controls of that service. Within 30 days after contract award, the Contractor shall provide to the Contracting Officer a list of all system administrator positions and personnel filling those positions, along with a schedule that ensures certification of all personnel within 90 days after contract award. Additionally, the Contractor should report all personnel changes which impact system administrator positions within 5 days of the personnel change and ensure these individuals obtain System Administrator certification within 90 days after the change.

(7) When the Contractor is located at a NASA Center or installation or is using NASA IP address space, the Contractor shall --

(i) Submit requests for non-NASA provided external Internet connections to the Contracting Officer for approval by the Network Security Configuration Control Board (NSCCB);

(ii) Comply with the NASA CIO metrics including patch management, operating systems and application configuration guidelines, vulnerability scanning, incident reporting, system administrator certification, and security training; and

(iii) Utilize the NASA Public Key Infrastructure (PKI) for all encrypted communication or non-repudiation requirements within NASA when secure email capability is required.

(c) Physical and Logical Access Requirements.

(1) Contractor personnel requiring access to IT systems operated by the Contractor for NASA or interconnected to a NASA network shall be screened at an appropriate level in accordance with NPR 2810 and Chapter 4, NPR 1600.1, NASA Security Program Procedural Requirements. NASA shall provide screening, appropriate to the highest risk level, of the IT systems and information accessed, using, as a minimum, National Agency Check with Inquiries (NACI). The Contractor shall submit the required forms to the NASA Center Chief of Security (CCS) within fourteen (14) days after contract award or assignment of an individual to a position requiring screening. The forms may be obtained from the CCS. At the option of NASA, interim access may be granted pending completion of the required

investigation and final access determination. For Contractors who will reside on a NASA Center or installation, the security screening required for all required access (e.g., installation, facility, IT, information, etc.) is consolidated to ensure only one investigation is conducted based on the highest risk level. Contractors not residing on a NASA installation will be screened based on their IT access risk level determination only. See NPR 1600.1, Chapter 4.

(2) Guidance for selecting the appropriate level of screening is based on the risk of adverse impact to NASA missions. NASA defines three levels of risk for which screening is required (IT-1 has the highest level of risk).

(i) IT-1 -- Individuals having privileged access or limited privileged access to systems whose misuse can cause very serious adverse impact to NASA missions. These systems include, for example, those that can transmit commands directly modifying the behavior of spacecraft, satellites or aircraft.

(ii) IT-2 -- Individuals having privileged access or limited privileged access to systems whose misuse can cause serious adverse impact to NASA missions. These systems include, for example, those that can transmit commands directly modifying the behavior of payloads on spacecraft, satellites or aircraft; and those that contain the primary copy of "level 1" information whose cost to replace exceeds one million dollars.

(iii) IT-3 -- Individuals having privileged access or limited privileged access to systems whose misuse can cause significant adverse impact to NASA missions. These systems include, for example, those that interconnect with a NASA network in a way that exceeds access by the general public, such as bypassing firewalls; and systems operated by the Contractor for NASA whose function or information has substantial cost to replace, even if these systems are not interconnected with a NASA network.

(3) Screening for individuals shall employ forms appropriate for the level of risk as established in Chapter 4, NPR 1600.1.

(4) The Contractor may conduct its own screening of individuals requiring privileged access or limited privileged access provided the Contractor can demonstrate to the Contracting Officer that the procedures used by the Contractor are equivalent to NASA's personnel screening procedures for the risk level assigned for the IT position.

(5) Subject to approval of the Contracting Officer, the Contractor may forgo screening of Contractor personnel for those individuals who have proof of a --

(i) Current or recent national security clearances (within last three years);

(ii) Screening conducted by NASA within the last three years that meets or exceeds the screening requirements of the IT position; or

(iii) Screening conducted by the Contractor, within the last three years, that is equivalent to the NASA personnel screening procedures as approved by the Contracting Officer and concurred on by the CCS.

(d) The Contracting Officer may waive the requirements of paragraphs (b) and (c)(1) through (c)(3) upon request of the Contractor. The Contractor shall provide all relevant information requested by the Contracting Officer to support the waiver request.

(e) The Contractor shall contact the Contracting Officer for any documents, information, or forms necessary to comply with the requirements of this clause.

(f) The Contractor shall insert this clause, including this paragraph (f), in all subcontracts when the subcontractor is required to –

(1) Have physical or electronic access to NASA's computer systems, networks, or IT infrastructure; or

(2) Use information systems to generate, store, or exchange data with NASA or on behalf of NASA, regardless of whether the data resides on a NASA or a contractor's information system.

(End of clause)

3. **RESERVED**

4. **RESERVED**

5. **RESERVED**

6. **RESERVED**

7. **RESERVED**

PART VI RESERVED

PART VII – CORE ATTACHMENTS

Attachment Number	Title	Dated	Number of pages
A	PRICE LIST FOR YEARS 1, 2, 3 (b)(4)		TBD
B	DATA REQUIREMENT DESCRIPTIONS	10/25/06	26
C	CORE STANDARD SOFTWARE LOAD	10/25/06	1
D	RESERVED	*	*
E	REVISED SEAT AND SERVICE LEVEL (REF Master Contract Attachment'E)	10/25/06	11

* To be incorporated by modification

Attachment A – PRICE LISTS

Incorporated as GSFC Price List (see Attachment A)

(b)(4)

ATTACHMENT B
DATA REQUIREMENT DESCRIPTIONS (DRD)

DRD NO.	DRD TITLE	DATED	PAGES
Core-1	Reports, Telephone Call (PCell and Mobile Computing) Detail	10/25/06	2
Core-2	Reports, Small Business Subcontracting	10/25/06	1
Core-3	Reports, Property Reporting	10/25/06	2
Core-4	Reports, Loss, Theft, Damage, and Destruction of Contractor Assets	10/25/06	1
Core-5	Reports, On-Site Contractor (Headcount)	10/25/06	1
Core-6	Reports, Move, Add, Change (M/A/C)	10/25/06	1
Core-7	Reports, Work Order Closure	10/25/06	2
Core-8	Reports, Standard Reporting for Security Incidents	10/25/06	1
Core-9	Reports, Help Desk Ticket Summary Report	10/25/06	1
Core-10	Reports, Security	10/25/06	1
Core-11	Plan, IT Security Program	10/25/06	2
Core-12	Reports, Lessons Learned Contingency	10/25/06	1
Core-13	RESERVED		
Core-14	RESERVED		
Core-15	RESERVED		
Core-16	RESERVED		
Core-17	RESERVED		

The following data descriptions are applicable to the type code set forth in the DRD documents identified above.

TYPE	DESCRIPTION
1	Data requiring written approval by the procuring activity prior to formal release for use or implementation.
2	Data submitted to procuring activity for review not later than 45 days prior to release for use or implementation. Data shall be considered approved unless the contractor has been notified of disapproval prior to target release date.
3	Data submitted to the procuring activity for coordination, surveillance, or information.
4	Data produced or used during performance of the contract and retained by the contractor to be made available to the procuring activity upon request. The contractor shall furnish a list to the procuring activity when requested to do so.
5	Data incidental to contract performance are to be retained by the contractor and reviewed by NASA upon request.

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION	**DATA REQUIREMENT DESCRIPTION**	**1. RFP #:** ODIN **2. DRD #:** Core-1 Page 1 of 2 Date: 10/25/06

3. TITLE: REPORTS, TELEPHONE CALL (PCell and Mobile Computing) DETAIL

SUBMITTAL REQUIREMENTS

4. TYPE: 3	**5. FREQUENCY OF SUBMISSION:** Monthly
6. DISTRIBUTION: Complete sets to Center DOCOTR with copy of transmittal letter to Center DOCO	**7. INITIAL SUBMISSION**: • One month after effective date of the delivery order • 10th business day of the month

8. REMARKS:
The Contractor shall provide all call detail records via CDROM, of all incoming and outbound calls, in support of security issues and tolls separation, verification and billing.

DATA REQUIREMENT DESCRIPTION

9. USE: The ODIN contractor shall maintain a record of the beginning and ending date and time of all telephone calls in electronic format on CDROM . This information shall be maintained by the ODIN contractor and made available to personnel as authorized by the DOCOTR.	**10. REFERENCE:** Part II, Section D **11. INTERRELATIONSHIP**: N/A

12. PREPARATION INFORMATION:

a. SCOPE:
Call detail records associated with a particular call shall be maintained on-line and, depending on traffic load and capabilities of the switch, downloaded on a regular schedule to CDROM for further separation and processing.

This information shall be maintained in such a way as to provide all inbound and outbound call details. Data file format shall be provided to authorized personnel to ensure interface compatibility with the NASA Management Information System.

Call detail records shall be handled in accordance with established Privacy Act regulations. Records shall be retained in accordance with NASA General Records Schedule and NASA NPR 1441.1C and any Center-specific guidelines pertaining to release of such information

b. CONTENTS:
The following fields of the Call Detail Records shall be required for all calls:

(1) Name assigned to the MC/PCell Seat
(2) Originating phone number
(3) Terminating (Destination) phone number (up to 15 digits)
(4) Destination number type (domestic, international, or unknown)

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION	**DATA REQUIREMENT DESCRIPTION**	1. **RFP #:** ODIN 2. **DRD #:** Core-1 Page 2 of 2 Date: 10/25/2006

3. TITLE: REPORTS, TELEPHONE CALL (PCell and Mobile Computing) DETAIL

DATA REQUIREMENT DESCRIPTION

12. PREPARATION INFORMATION: (continued)

CONTENTS (continued)

(5) Length of Call (minutes: seconds)
(6) Time of call (hour:minutes)
(7) Month/day/year of call
(8) City, State, Country Called
(9) Organization Code assigned to the Calling Number
(10)Date/Time Period covered by Report

Additional Reporting Requirement

(1) Video Streaming usage
(2) Multimedia messaging usage
(3) Text messaging usage

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

DATA REQUIREMENT DESCRIPTION (DRD)

1. RFP #: ODIN
2. DRD #: Core-2
Page 1 of 1
Date: 10/25/2006

3. TITLE: REPORTS, SMALL BUSINESS SUBCONTRACT REPORTING

SUBMITTAL REQUIREMENTS

4. TYPE: 3

5. FREQUENCY OF SUBMISSION:

Report is due 30 days after the close of each reporting period.

Standard Form (SF) 294: Semi-Annually

Form	Reporting Period
SF 294	October 1 – March 31
SF 294	April 1 – September 30

6. DISTRIBUTION:
Via eSRS: No further distribution required.
Via Hardcopy:
1 - Center DOCO
1 - Center Small Business Officer

7. INITIAL SUBMISSION: N/A

8. REMARKS:
Once the eSRS system is operational the Contractor shall submit the report electronically, the Government will notify the Contractor once this system is operational.

DATA REQUIREMENT DESCRIPTION

9. USE:
To obtain center-specific data for small and large business dollars spent under the Delivery Order.

10. REFERENCE:

- FAR “Small Business Subcontracting Plan” 52.219-9

11. INTERRELATIONSHIP: N/A

12. PREPARATION INFORMATION:

The data/goals on the SF-294 shall be specific to each delivery order.

If submitting via hard copy, this form shall be prepared in accordance with the instructions contained on the back of the SF-294 form.

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION	**DATA REQUIREMENT DESCRIPTION (DRD)**	**1. RFP #:** ODIN **2. DRD #:** CORE-3 Page 1 of 2 Date: 10/25/2006

3. TITLE: REPORTS, PROPERTY REPORTING

SUBMITTAL REQUIREMENTS

4. TYPE: 3	**5. FREQUENCY OF SUBMISSION:** • Monthly, on the 10th business day the Month • For loss or theft of equipment, the DOCOTR or designee will receive immediate (within 2 hours) verbal notification at time of incident discovery. • After verbal notification of loss or theft, an interim written report will be provided within 24 hours of incident discovery to the DOCOTR or designee
6. DISTRIBUTION: Via E-mail: - Center DOCO - Center DOCOTR	**7. INITIAL SUBMISSION:** • 10th business day of the month • Upon loss or theft of equipment, the DOCOTR or designee will receive immediate verbal notification at time of incident discovery.

8. REMARKS: The Contractor shall develop and maintain records to substantiate both the nature of property losses and reimbursement costs, and to document Contractor-owned assets brought on-site and disposed for Stevenson-Wydler Act activities.

DATA REQUIREMENT DESCRIPTION

9. USE: To monitor property owned and managed by the ODIN Contractor, including Contractor-owned assets that are lost, stolen, or damaged.	**10. REFERENCE:** • Master Contract, Paragraph A.1.20 (Liability) • Master Contract, Paragraph C.5.6 (Asset Requirements) • Master Contract, Paragraph C.3.2.2 (Stevenson-Wydler Act)) **11. INTERRELATIONSHIP:** N/A

12. PREPARATION INFORMATION:
The Contractor shall report property data for each delivery order separately, including, at a minimum, the following, in a single, complete submission:

a. Contractor-provided assets provided to the Government in performance of this delivery order that are lost, stolen, damaged, or destroyed, including, but not limited to:
   - Identification of the item by description and inventory number
   - Name of the employee to whom the equipment was assigned
   - Center-specific organization to which equipment was assigned
   - Date of the event
   - Nature of loss (loss, theft, damage, or destruction)
   - Brief explanation of what happened/where/how it was lost or damaged

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION	**DATA REQUIREMENT DESCRIPTION (DRD)**	**1. RFP #:** ODIN **2. DRD #:** CORE-3 Page 2 of 2 Date: 10/25/2006

3. TITLE: REPORTS, PROPERTY REPORTING

12. PREPARATION INFORMATION: (Continued)

- Dollar amount of loss
- Basis for actual loss value (acquisition cost less depreciation, or replacement cost)
- Age of the item
- Cumulative dollar amount of losses per contract year
- Total dollar amount for the cumulative Delivery Order

13. New property brought on Center, including tech refresh and direct purchase items (i.e., incoming ODIN-owned inventory) and associated inventory numbers.

14. Catalog-purchased items, by organization, delivered during the reporting period.

ODIN-owned property disposed for Stevenson-Wydler Act activities, including the items, their depreciated value, and to which schools, and verification that any drives were erased first.

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION	**DATA REQUIREMENT DESCRIPTION**	1. **RFP #:** ODIN 2. **DRD #:** Core-4 Page 1 of 1 Date: 10/25/2006

3. TITLE: REPORTS, LOSS, THEFT, DAMAGE, AND DESTRUCTION OF CONTRACTOR ASSETS

SUBMITTAL REQUIREMENTS

4. TYPE: 3	**5. FREQUENCY OF SUBMISSION:** 10th business day of each month or unless otherwise instructed by DOCO, DOCOTR or Center ITSM
6. DISTRIBUTION: Complete sets to Center DOCO, DOCOTR and Center ITSM	**7. INITIAL SUBMISSION:** 10th business day of month

8. REMARKS: The Contractor shall develop and maintain records to substantiate both the nature of the loss and the reimbursement costs.

DATA REQUIREMENT DESCRIPTION

9. USE: Provides NASA with detailed data supporting the nature of the loss and the reimbursement costs of contractor-owned assets.	**10. REFERENCE:** Master Contract A.1.20, Liability
	11. INTERRELATIONSHIP:

12. PREPARATION INFORMATION:

a. The Contractor shall submit the data for each delivery order separately.

b. The Contractor shall report all losses of contractor-provided assets provided to the Government in performance under this delivery order.

c. The Contractor shall ask the user if the information on the affected system is SBU.

d. As a minimum, the report shall include the following data:
(1) Nature of loss (loss, theft, damage, or destruction)
(2) Date of event
(3) Description of what happened
(4) Basis for actual loss value (acquisition cost less depreciation or replacement cost)
(5) Dollar amount of loss
(6) Cumulative dollar amount per contract year
(7) If SBU data, list the class of data as indicated in Section 5.24 of NPR 1600.1 (i.e., ITAR, procurement sensitive, PII, propriety, etc….).

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

DATA REQUIREMENT DESCRIPTION

1. **RFP #:** ODIN
2. **DRD #:** Core-5

Page 1 of 1

Date: 10/25/2006

3. TITLE: REPORTS, ON-SITE CONTRACTOR (HEADCOUNT)

SUBMITTAL REQUIREMENTS

4. TYPE: 3

5. FREQUENCY OF SUBMISSION: Monthly

6. DISTRIBUTION: 1 complete set (hardcopy) to Center DOCO and electronically to Center DOCO, DOCOTR, and Alternate DOCOTR

7. INITIAL SUBMISSION: 10th business day after Delivery Order start date

8. REMARKS: Contractor shall provide information in accordance with Block 12.

DATA REQUIREMENT DESCRIPTION

9. USE: Onsite Contractor report used for various security and physical access to facility requirement.

10. REFERENCE: N/A

11. INTERRELATIONSHIP: N/A

12. PREPARATION INFORMATION:

a. The Contractor shall report each Center separately.

b. The Contractor shall report the number of ODIN on-site employees (headcount) by company. This includes all ODIN subcontractors, if on-site.

c. The report shall include the following information for each employee: employee's name, position, location (building/room number), shift assignment, supervisor's name, and supervisor's location (building/room number).

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION	**DATA REQUIREMENT DESCRIPTION**	1. **RFP #:** ODIN 2. **DRD #:** Core-6 Page 1 of 1 Date: 10/25/2006

3. TITLE: REPORTS, MOVE, ADD, CHANGE (M/A/C)

SUBMITTAL REQUIREMENTS

4. TYPE: 2	**5. FREQUENCY OF SUBMISSION:** 10th business day of each month
6. DISTRIBUTION: Complete sets to Center DOCO and DOCOTR	**7. INITIAL SUBMISSION:** 10th business day after Delivery Order start date

8. REMARKS: The Contractor shall track and report the quantity of M/A/C performed.

DATA REQUIREMENT DESCRIPTION

9. USE: Provides NASA with the quantity of M/A/C actions for user requested system hardware de-installation, move and re-installation of catalog hardware and software.	**10. REFERENCE:** Master Contract Section E.3.1.8 Delivery Order Part II Section A.8.b.
	11. INTERRELATIONSHIP: N/A

12. PREPARATION INFORMATION:

a. The contractor shall report the number of M/A/C during the month for each Delivery Order.

b. This data shall be provided electronically and shall be reported by major organization by major seat type, e.g. desktop, phone, etc.

c. The Contractor shall include a complete listing of all M/A/C actions to support the number reported for the month.

d. The report shall show the number of M/A/C performed during the month and the cumulative contract year-to-date totals.

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION	**DATA REQUIREMENT DESCRIPTION**	1. **RFP #:** ODIN 2. **DRD #:** Core-7 Page 1 of 2 Date: 10/25/2006

3. TITLE: REPORT, WORK ORDER CLOSURE

SUBMITTAL REQUIREMENTS

4. TYPE: 3	**5. FREQUENCY OF SUBMISSION:** Weekly
6. DISTRIBUTION: Complete sets to Center DOCO and DOCOTR	**7. INITIAL SUBMISSION:** One week after the Delivery Order period of performance start date

8. REMARKS: The contractor shall provide closure information for submitted orders, Technology refreshments, trouble tickets, Return to Service (RTS), and Error changes by next Close of Business day in which the work was performed.

DATA REQUIREMENT DESCRIPTION

9. USE:
Closure information will be used to update NASA Management Information Systems databases in timely manner.

10. REFERENCE:

- Master Contract C.5.3
- Delivery Order, Section G – Help Desk

11. INTERRELATIONSHIP:

12. PREPARATION INFORMATION:

a. The Contractor shall provide the information for each delivery order.

b. Daily closure report for orders submitted to the ODIN contractor shall provide the following information, as applicable:
   (1) The center issued order number
   (2) The associated ODIN database tracking number
   (3) Configuration information modifications that resulted from the issued order
   (4) Date of completion (closure)

c. Daily closure information for Hardware Technology Refreshments shall include:
   (1) The order number, if applicable
   (2) The Equipment tag number (ECN) of the replaced equipment
   (3) The Equipment tag number (ECN) of the replacement equipment
   (4) Original date scheduled for replacement
   (5) Date the equipment was replaced
   (6) The assigned ODIN database tracking number

d. Daily closure information for Trouble Tickets shall include:
   (1) A daily report of closed trouble tickets that resulted in changes to:
   (2) Equipment tag numbers
   (3) Location changes, including but not limited to Port numbers, Building locations
   (4) Service Level Changes
   (5) ODIN ticket associated with the Trouble Ticket

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION	**<u>DATA REQUIREMENT DESCRIPTION</u>**	**1. RFP #:** ODIN **2. DRD #:** Core-7 Page 2 of 2 Date: 10/25/2006

3. TITLE: REPORT, WORK ORDER CLOSURE

DATA REQUIREMENT DESCRIPTION

12. PREPARATION INFORMATION <u>(continued)</u>

e. The DOCOTR or designee must approve error Changes.

f. Daily closure information for Return to Service (RTS) shall provide:
   (1) Copy of trouble ticket identifying the RTS
   (2) The assigned ODIN database tracking ticket associated with the RTS

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION	**DATA REQUIREMENT DESCRIPTION**	1. **RFP #:** ODIN 2. **DRD #:** Core-8 Page 1 of 1 Date: 10/25/2006

3. TITLE: REPORTS, STANDARD REPORTING FOR SECURITY INCIDENTS

SUBMITTAL REQUIREMENTS

4. TYPE: 2	**5. FREQUENCY OF SUBMISSION:** IAW Center ITSM requirements and on request
6. DISTRIBUTION: Complete sets to Center DOCO, DOCOTR and NASA IT Security Manager	**7. INITIAL SUBMISSION**: 30 days after the Delivery Order period of performance start date

8. REMARKS:

DATA REQUIREMENT DESCRIPTION

9. USE:
Report to ITSM and as requested to Inspector General on Virus Damage Assessment Inspector General

10. REFERENCE:

- Master Contract C.8, Information Technology Security Requirement
- NPR 1600.1

11. INTERRELATIONSHIP:

12. PREPARATION INFORMATION:

SCOPE: The Contractor shall report the significant security breach incidents as defined in NPR 2810.1*x* (Chapter 17 Security Incident Handling and Reporting).

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION	**DATA REQUIREMENT DESCRIPTION**	**1. CONTRACT #:** ODIN **2. DRD #:** Core-9 Page 1 of 1 Date: 10/25/2006

3. TITLE: REPORT, HELP DESK TICKET SUMMARY

SUBMITTAL REQUIREMENTS

4. TYPE: 3	**5. FREQUENCY OF SUBMISSION:** Monthly, on the 10th business day of each month.
6. DISTRIBUTION: DOCO, DOCOTR, & Others as designated by DOCOTR	**7. INITIAL SUBMISSION:** 10th business days after the end of the month in which the delivery order starts.

8. REMARKS:
The Contractor shall generate, maintain, and submit a monthly summary report of all help desk tickets.

DATA REQUIREMENT DESCRIPTION

9. USE: To identify trends and provide corrective actions where needed.	**10. REFERENCE:** Core Part II, Section G – Help Desk Section
	11. INTERRELATIONSHIP: N/A

12. PREPARATION INFORMATION:

This summary report shall include an accumulation of all help desk tickets for each month. The report shall be in spreadsheet format, with at least the following descriptive information and as many additional columns as needed to relay appropriate data for each partial and complete month in the delivery order.

a. Request Type – to indicate whether the work request was for ODIN or non-ODIN service. Additional breakout of the non-ODIN types may be added as identified and/or approved by the DOCOTR.
b. Type of Service – to indicate the general type of work required, e.g., Account Administration, Maintenance, Asset Management, etc.
c. Category – to provide more specific information about the type of service required, e.g., Desktop M/A/C, Phone Service, Hardware, Password Reset, Home Use Software, etc.
d. Help Desk Ticket Number
e. Ticket Initiation Date/Time
f. Ticket Resolution Due Date/Time
g. Ticket Status as of reporting date
h. Seat ID/ODIN Tag Number
i. User Name
j. User Organization Code
k. Metric Evaluation – indication, for closed tickets, whether service metric was met or missed (Pass/Fail)

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION	**DATA REQUIREMENT DESCRIPTION**	1. **Contract:** ODIN 2. **DRD #:** Core-10 Page 1 of 1 Date: 10/25/2006

3. TITLE: REPORTS, SECURITY

SUBMITTAL REQUIREMENTS

4. TYPE: 1

5. FREQUENCY OF SUBMISSION: At least once every three years or upon significant change to the functionality of the assets, network connectivity, or mission of the system, whichever comes first. (see remarks)

6. DISTRIBUTION: Complete sets to Center DOCO, DOCOTR and Center IT Security Manager, or designee

7. INITIAL SUBMISSION: 45 days after the effective date of the Delivery Orders.

8. REMARKS:
If the Contractor discovers new or unanticipated threats or hazards, or if existing safeguards have ceased to function effectively, the Contractor shall update the risk assessments and IT Security Plans (within 30 working days).

DATA REQUIREMENT DESCRIPTION

9. USE:
The ODIN contractor shall provide risk assessments and IT Security Plans to the Government for approval.

The ODIN contractor shall maintain this information and make it available to applicable Center IT Security Manager or designee, if requested.

10. REFERENCE:
C.8

11. INTERRELATIONSHIP:
C.8.3, C.8.4, C.8.6

12. PREPARATION INFORMATION:

a. **SCOPE:**
The Contractor shall conduct initial risk assessments, document the results, develop and maintain IT Security Plans in accordance with the IT security requirements in effect at the Center at which the system is operated.

b. **CONTENTS:**
The IT Security Plans shall describe how the integrity, availability, confidentiality of the information and IT resources will be protected, including protection (disclosure) from the subject contractor.

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION	**DATA REQUIREMENT DESCRIPTION (DRD)**	**1. RFP #:** ODIN **2. DRD #:** Core-11 Page 1 of 2 Date: 10/25/2006

3. TITLE: PLAN, IT SECURITY PROGRAM

SUBMITTAL REQUIREMENTS

4. TYPE: 1	**5. FREQUENCY OF SUBMISSION:** Plan shall be updated and submitted within 30 calendar days of significant change to the functionality of the assets, network connectivity, or mission of the system; if new or unanticipated threats or hazards are discovered; or if the CITSM or Contractor determine that existing safeguards have ceased to function effectively.
6. DISTRIBUTION: Via E-mail to: - Center DOCO - Center DOCOTR - Center IT Security Manager	**7. INITIAL SUBMISSION:** Plan shall be submitted within 45 calendar days after Delivery Order start date. This plan, as approved by the DOCO, shall be incorporated into the Delivery Order as a compliance document.

8. REMARKS: The IT Security Program Plan is critical for performance of this Delivery Order. Upon receipt of this Plan, the Government will review and provide comment back to the Contractor of any recommended or required changes.

Following approval of the Plan or revisions thereto by the DOCO, this Plan shall be followed completely by the Contractor in the performance of its work.

DATA REQUIREMENT DESCRIPTION

9. USE: To ensure compliance with federal, agency, and local IT security requirements and to monitor IT security related issues.	**10. REFERENCE:** • NFS Clause 1852.204-76 (Ref. to Master Contract) • Current version of NPR 2810.1*x* • Master Contract paragraph, C.8, Information Technology Security Requirements **11. INTERRELATIONSHIP:**

12. PREPARATION INFORMATION:
See Chapter 5 of the NASA Procedural Requirements (NPR) 2810.*x* (Security of Information Technology) and ITS SOP-0018 for information required in this plan.

NOTE: To review this manual in its entirety, see the NASA Online Directives Information System (NODIS) Library at the following URL:
http://nodis3.gsfc.nasa.gov/Library/main_lib.html

A separate plan for each delivery order shall be provided to the appropriate Center, and shall include, at a minimum:

a. An initial risk assessment, documentation of results, and resultant IT Security Plan(s) in accordance with the IT security requirements in effect at the Center.

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION	**DATA REQUIREMENT DESCRIPTION (DRD)**	**1. RFP #:** ODIN **2. DRD #:** Core-11 Page 2 of 2 Date: 10/25/2006

3. TITLE: PLAN, IT SECURITY PROGRAM

12. PREPARATION INFORMATION: (continued)

b. Description of how the integrity, availability, and/or confidentiality of information and IT resources will be protected, including protection (disclosure) from the subject contractor. IT resources include, but are not limited to:

- i. Desktop Systems
- ii. Server Servers
  - a. Public and secure (as defined by NPR 2810.*x*) Web servers
  - b. Electronic messaging (E-mail and directory services) servers
  - c. Other servers providing Center-wide services to or at the Center.

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION	**DATA REQUIREMENT DESCRIPTION (DRD)**	1. **RFP #:** ODIN 2. **DRD #:** Core-12 Page 1 of 1 Date: 10/25/2006

3. TITLE: REPORTS, LESSONS LEARNED CONTINGENCY

SUBMITTAL REQUIREMENTS

4. TYPE: 3	**5. FREQUENCY OF SUBMISSION:** 30 days after triggering event or 30 days after mishap investigation or hazard analysis / evaluation is completed.
6. DISTRIBUTION: Center DOCO and DOCOTR	**7. INITIAL SUBMISSION:** Center Occupational Safety Branch (1 electronic copy including photographs, drawings, etc., in web-ready format such as HTML or JPG) and DOCOTR (1 copy)

8. REMARKS:

Obtains Lessons learned from Contractor for possible publication in NASA Lessons Learned Information System (LLIS).

The Office of Primary Responsibility for this DRD is the Center Safety, Reliability, and Quality Assurance Office.

DATA REQUIREMENT DESCRIPTION

9. USE: Provide NASA with innovative ideas of future products/solutions for technology infusion.	**10. REFERENCE:** • Current version of NPG 2810.1*x* • NPG 8715.3 (as revised) • JPG 1700.1 (as revised)
	11. INTERRELATIONSHIP:

12. PREPARATION INFORMATION:

Criteria for Selecting Lessons Learned. Uncommon insight arising from any event or observation that will benefit from sharing with a larger community of interested parties. Lessons learned are intended to prevent recurrence of undesirable events and to allow NASA and its team members to capitalized to the greatest extent practical on unique successes.

Content:
Subject - one line subject of the lesson.
Lesson Learned - usually one sentence that describes insight gained
Description of Event - narrative of what happened.
Recommendations - may be an action plan, suggestion, etc., that was adopted at event source.
Supporting documentation - as needed to give clear picture of lesson (photographs, illustrations, drawings, etc.)
Contact name and e-mail address (for follow up by Government prior to publication of lesson)
Definitions. Refer to NASA LLIS at http://llis.gsfc.nasa.gov/ for definitions of terms used.

ATTACHMENT C
CORE STANDARD SOFTWARE LOAD

Core Standard Software Load					
				Standard Load	
Application	*Settings*	*Windows*	*Mac*	*Windows*	*Mac*
ActivClient	TBD	X	X	TBD	TBD
Adobe Acrobat Reader	Customized Install (removes updater and EULA)	X	X	7.X	7.X
Authorware Web Player	Factory	X	X	2004.0.0.73	7
Entrust Entelligence & required plug-ins	Site INI file	X	X	7.X	7.X
Firefox Web Browser	Customized config file per site	X	X	1.5.X	1.5.X
Flash Player	Factory	X	X	8.X	8.X
Internet Explorer	Factory	X		6.X	
Java run-time environment	Factory	X	X	1.4	1.4
Macintosh Operating System	CIS Template (NASA to define least common denominator - GRC recommended config)		X		10.4.6
Microsoft Office (Professional Edition with Outlook)	Site specific entries customized via Registry entry for AIP	X		2003 SP2	
Microsoft Office for MAC	Factory		X		2004 SP
MS Entourage	Factory		X		2004 SP
Symantec Antivirus	Site GRC.DAT file	X	X	10.X	10.X
PatchLink (Update)	Site configuration for Server info	X	X	Latest Version Provided	Latest Version Provided
Quicktime	Factory	X	X	7	7
Realplayer/RealOne Basic	Factory	X	X	10	10
Shockwave	Factory	X	X	10.X	10.X
Stuff-It Standard	Factory		X		10
Timbuktu (TBD – if at currently at use at all the centers)	Site Key	X	X		
Windows Media Player	Factory	X		10	
Windows Operating System	CIS Template (NASA to define least common denominator - GRC recommended config)	X		XP Pro sp2	
Windows Messenger	Enterprise LCS Settings	X	X	Communicator 2005	5.1.1
Winzip	Factory	X		9.X	9.X
Citrix ICA Client	Factory	x	x		
FileNet Desktop E-Forms	Factory	x	x	4.2	4.2
FetchFTP	Factory		x		5.0.5
Flip4Mac Media Component (media player for Windows Media Player file)	Factory		x		2
Safari	Factory		x		
X.509 Root Certificates	Factory	x	x		
Factory under Settings means the application is installed choosing the defaults for all settings. For any item that is not set to factory defaults a site overlay script can be used to deploy the required changes.					
Note: The software listed does not take into account whether the software licenses are provided by the Government or the Contractor and is only for the purposes of establishing core apps and their settings for the load					

ATTACHMENT D

(RESERVED)

ATTACHMENT E
SUMMARY OF SEATS AND SERVICE LEVELS FOR DESKTOPS
(Reference: Master Contract Table E.2.1.1)

TABLE E-1 SUMMARY OF SEATS AND SERVICE LEVELS FOR COMPUTER SEATS
(Reference: Master Contract Table E.2.1.1)

Seat Types	DESKTOP	LAPTOP	WORKSTATION	WORKSTATION UNIX	MA1	MA2	MA MISC	NAD
Architecture								
Windows	S	S	S					
MAC	O	O	O					
Linux	O	O	O					
HP (UNIX Only)				O				
SUN (UNIX Only)				S				
SGI (UNIX Only)				O				
Platform								
Standard	S	S	S					
Lightweight		O						
Tablet		O						
Entry (UNIX Only)				S				
Mid (UNIX Only)				O				
High (UNIX Only)				O				
Processor								
Regular			S					
Enhanced			O					
Docking Station								
No ODIN Supplied		O						
None		S		S				
Basic		O						
Monitor								
None	O	O	O	O				
Basic	O	O	O	O				
Regular	S	S	S	S				
Premium	O	O	O	O				
Enhanced	O	O	O	O				
Critical	O	O	O	O				
ODIN Application Software								
None	O	O	O	S				S
Standard	S	S	S	O				O
Hardware Maintenance								
None	O	O	O	O				S
Basic	O	O	O	O	O	O		O
Regular	S	S	S	S	S	S		O
Premium	O	O	O	O	O	O		O
Enhanced	O	O	O	O	O	O		O
Critical	O	O	O	O	O	O		O

Seat Types	DESKTOP	LAPTOP	WORK-STATION	WORK-STATION UNIX	MA1	MA2	MA MISC	NAD
System Software Maintenance								
None	O	O	O	O				S
Basic	O	O	O	O				O
Regular	S	S	S	S				O
Premium	O	O	O	O				O
Enhanced	O	O	O	O				O
Critical	O	O	O	O				O
ODIN-Appl Software Maintenance								
None	O	O	O	O				S
Basic	O	O	O	O				O
Regular	S	S	S	S				O
Premium	O	O	O	O				O
Enhanced	O	O	O	O				O
Critical	O	O	O	O				O
Hardware Tech Refresh								
Basic	O	O	O	O				
Regular	O	O	O	O				
Premium	S	S	S	S				
Enhanced	O	O	O	O				
Software Tech Refresh								
Regular	S	S	S	S				
Enhanced	O	O	O	O				
Moves, Adds, Changes								
Regular	S	S	S	S	S	S	S	S
Enhanced	O	O	O	O	O	O	O	O
LAN Services								
No ODIN supplied network connection	O	O	O	O	O	O	O	O
Standalone	O	O	O	O	S	S	S	
Basic LAN	S	S	S	S				S
Remote-S LAN access	O	O	O	O				O
Remote-W LAN access		O						O
Remote-C		O						
Remote-S & Basic LAN		O						O
Remote S & Remote W & Basic LAN		O						O

Seat Types	DESKTOP	LAPTOP	WORK-STATION	WORK-STATION UNIX	MA1	MA2	MA MISC	NAD
access								
Remote S & Remote-W & Remote-C & Basic LAN Access		O						
Fast LAN	O	O	O	O				O
Huge LAN	O		O	O				O
Integrated Customer Support / Help								
Basic	O	O	O	O	O	O	O	O
Regular	S	S	S	S	S	S	S	S
Enhanced	O	O	O	O	O	O	O	O
Training								
None	O	O	O	O	S	S	S	S
Basic	S	S	S	S				O
System Administration								
Basic	O	O	O	S	S	S	S	S
Regular	S	S	S	O	O	O	O	O
Enhanced	O	O	O	O	O	O	O	O
Shared Peripheral Services								
None	O	O	O	O	S	S	O	S
Basic	S	S	S	S			S	O
Regular	O	O	O	O			O	O
Enhanced	O	O	O	O			O	O
Critical	O	O	O	O			O	
File services								
None	O	O	O	O	S	S	S	S
Basic	S	S	S	S				O
Regular	O	O	O	O				O
Enhanced	O	O	O	O				O
Local Data Backup and Restore Services								
None	O	O	O	O	S	S	S	S
Basic	S	S	S	S				O
Regular	O	O	O	O				O
Enhanced	O	O	O	O				O
Desktop Conferencing								
None	S	S	S	S	S	S	S	S
Basic	O	O	O	O				

Seat Types	**DESKTOP**	**LAPTOP**	**WORK-STATION**	**WORK-STATION UNIX**	**MA1**	**MA2**	**MA MISC**	**NAD**
Enhanced	O	O	O	O				
Account Services								
None	O	O	O	O				O
Basic	S	S	S	S				S
E-Mail Services								
None	O	O	O	O				O
Basic	S	S	S	S				S
E-mail Storage Services								
None	O	O	O	O				O
Basic	S	S	S	S				S
Regular	O	O	O	O				O
Enhanced	O	O	O	O				O
Laptop Loaner Pool Management								
None		S		S				
Basic		O						
Print Queue Services								
None					S	S	S	
Regular					O	O	O	
Color Services								
None							S	
Regular							O	

TABLE E-2 SUMMARY OF SEATS AND SERVICE LEVELS FOR DESKTOPS
(Reference: Master Contract Table E.2.1.1)

(Account Seats)

Seat Type	ACCOUNT
Account Services	
None	O
Standard	S
E-mail Services	
None	O
Standard	S
E-mail Storage Services	
None	O
Basic	S
Regular	O
Enhanced	O
Premium	O
File Storage Services	
None	S
Basic	O
Regular	O
Enhanced	O
Premium	O

TABLE E-3 – SUMMARY OF SEATS AND SERVICE LEVELS FOR MOBILE COMPUTING

Seat Type	**MC**
Architecture	
MC1	S
MC2	O
MC3	O
Hardware Refreshment	
Basic	S
Regular	
Premium	
Enhanced	O
Critical	O
Service Plan	
Data Only	O
Basic	O
Regular	S
Premium	O
Enhanced	O
Critical	O
Text Messaging	
None	S
Basic	O
Regular	O
Premium	O
Enhanced	O
Critical	O
Voice Mail	
None	O
Basic	S
Regular	O
Premium	
Enhanced	
Critical	
Hardware Maintenance	
Basic	O
Regular	O
Premium	S
Enhanced	O
Critical	O
System Software Maintenance	
Basic	O
Regular	O
Premium	S
Enhanced	O

Critical	O
Software Technology Refreshment	
Basic	O
Regular	S
Premium	
Enhanced	
Critical	
Integrated Help Desk Support	
Basic	O
Regular	S
Premium	
Enhanced	O
Critical	
Calling Plan	
Domestic	S
International	O
Return to Service	
Premium	S
Enhanced	O
Critical	O
Moves, Add, Changes	
Regular	S
Enhanced	O

TABLE E-4 - SUMMARY OF SEATS AND SERVICE LEVELS FOR SERVERS
(Reference: Master Contract Table E.2.2.1)

Server Service Type	WEB1	APP1	FILE1	SERV1	SERV2
Platform Architecture					
None					S
Windows				S	
UNIX				O	
MAC				O	
System Administration					
Regular	O	O	O	S	O
Enhanced	S	S	S	O	S
Maintenance					
Regular	O	O	O	O	O
Premium	O	O	O	O	O
Enhanced	S	S	S	S	S
Critical	O	O	O	O	O
Storage Volume					
None					S
Basic	S	O	O		
Regular	O	S	S		
Premium	O	O	O		
Enhanced	O	O	O	S	
Critical				O	
Data Backup and Restoration					
None	O	O	O	O	O
Basic	O	O	O	O	O
Regular	S	S	S	S	S
Enhanced	O	O	O	O	O
Performance Delivery					
Basic	O	O	O		
Regular	S	S	S	S	
Premium	O	O	O	O	
Enhanced	O	O	O	O	
Security Features					
None	S	S	S	S	S
Basic	O	O	O	O	O
Regular	O	O	O	O	O
Enhanced	O	O	O	O	O
Server Location					
Regular				S	O
Enhanced				O	S

TABLE E-5 – SUMMARY OF SEATS AND SERVICE LEVELS FOR PHONE SERVICE
(Reference Master Contract Table E.2.3.1)

Seat Type	PCell
Instrument	
Regular	S
Premium	O
Hardware Refreshment	
Basic	O
Regular	
Premium	
Enhanced	S
Critical	O
Service Plan	
Basic	O
Regular	S
Premium	O
Enhanced	O
Critical	O
Text Messaging	
None	S
Basic	O
Regular	O
Premium	O
Enhanced	O
Critical	O
Voice Mail	
None	O
Basic	S
Regular	O
Premium	
Enhanced	
Critical	
Hardware Maintenance	
Basic	O
Regular	O
Premium	S
Enhanced	O
Critical	O
Integrated Help Desk Support	
Basic	O
Regular	S
Premium	
Enhanced	O

Critical	
Calling Plan	
Domestic	S
International	O
Moves, Add, Changes	
Regular	S
Enhanced	O

TABLE E-6 – SUMMARY OF SEATS AND SERVICE LEVELS FOR VIRTUAL TEAM MEETING (VTM)

Seat Type	VTM
Small	S
Medium	O
Large	O
Extra Large	O
Unlimited	O

End Table